WHAT IS CLAIMED IS:

1. A method of securely communicating confidential information among at least three consenting parties, said method comprising:

establishing a relationship among the parties;

creating a document initiated by one of the parties;

adding verifying information to said document about each of the parties to said document in order to validate said document;

adding an expiration time to said document in order to validate said document;

at least one of the parties presenting said document to at least one other of the parties prior to communication of the confidential information therebetween; and

said other of the parties permitting said communication of the confidential information therebetween only if said document is valid and said expiration time has not passed.

2. A method according to claim 1, wherein at least two of the parties add respective preselected expiration times to said document in order to validate said document, said other of the parties permitting said communication therebetween only if the earliest expiration time has not passed.

3. A method according to claim 1, wherein at least a portion of said document is encrypted.

4. A method according to claim 3, wherein at least a portion of said document is symmetrically encrypted.

5. A method according to claim 3, wherein at least a portion of said document is asymmetrically encrypted.

6. A method according to claim 1, wherein said document includes a digital signature of each of the parties.

7. A method according to claim 3, wherein said encrypted information is capable of decryption using an encryption key.

8. A method according to claim 7, wherein said encryption key is a public key.

9. A method according to claim 7, wherein said encryption key is a private key.

10. A method according to claim 9, wherein said private key is a multiple-use key.

11. A method according to claim 9, wherein said private key is a one-time use key.

12. A method according to claim 3, wherein said encrypted information is encrypted with a public key and capable of decryption using a private key.

13. A method of securely communicating confidential information among at least three parties, said method comprising:

establishing an electronic communication relationship among all the parties;

creating an electronic ticket initiated by a first of the parties;

adding security information pertaining to said first party to said electronic ticket and then sending said electronic ticket to a second of the parties;

adding security information pertaining to said second party to said electronic ticket and then sending said electronic ticket to a third of said parties;

adding security information pertaining to said third party to said electronic ticket;

validating said electronic ticket by verifying said security information pertaining to said at least three parties;

at least one of the parties presenting said electronic ticket to another of the parties prior to communicating confidential information therebetween; and

said other of the parties permitting said communication of confidential information therebetween only after said electronic ticket is validated.

14. A method according to claim 13, wherein at least part of said security information pertaining to at least two of the respective parties is symmetrically encrypted.

15. A method according to claim 13, wherein at least part of said security information pertaining to at least two of the respective parties is asymmetrically encrypted.

16. A method according to claim 13, wherein said electronic ticket includes a digital signature of at least one of the respective parties.

17. A method according to claim 13, wherein said encrypted security information pertaining to at least one of the respective parties is capable of decryption using an encrypted key.

18. A method according to claim 17, wherein said encryption key is a public key.

19. A method according to claim 17, wherein said encryption key is a private key.

20. A method according to claim 19, wherein said private key is a multiple-use key.

21. A method according to claim 19, wherein said private key is a single use key.

22. A method according to claim 13, wherein each of the parties has a digital certificate, said respective parties each digitally signing said electronic ticket.

23. A method according to claim 13, wherein at least one of the parties adds a preselected expiration time to said electronic ticket, said other of the parties permitting said communication of confidential information therebetween only if said expiration time has not passed.

24. A method according to claim 13, wherein at least two of the parties add respective preselected expiration times to said document in order to validate said document, said other of the parties permitting said communication therebetween only if the earliest expiration time has not passed.

25. A method of electronically communicating secure confidential information among at least three parties, said method comprising:

establishing an electronic communication relationship among all the parties;

creating an electronic ticket initiated by a first of the parties;

adding a digital signature of the first party and encrypted security information pertaining to the first party to said electronic ticket;

adding a digital signature of the second party and encrypted security information pertaining to the second party to said electronic ticket;

adding a digital signature of the third party and encrypted security information pertaining to the third party to said electronic ticket;

validating said electronic ticket by verifying said security information pertaining to said at least three parties;

at least one of the parties presenting said electronic ticket to another of the parties prior to communicating confidential information therebetween; and

said other of the parties permitting said communication of confidential information therebetween only after said electronic ticket is validated.

26. A method according to claim 25, wherein at least one of the parties adds a preselected expiration time to said electronic ticket in order to validate said electronic ticket, said other of the parties permitting said communication of confidential information therebetween only if said expiration time has not passed.

27. A method according to claim 25, wherein at least two of the parties add respective preselected expiration times to said electronic ticket in order to validate said electronic ticket, said other of the parties permitting said communication of confidential information therebetween only if the earliest of said expiration times has not passed.

28. A method according to claim 25, wherein at least part of said electronic ticket is symmetrically encrypted.

29. A method according to claim 25, wherein at least part of said electronic ticket is asymmetrically encrypted.

30. A method for a first party to securely communicate confidential information of at least a second party with at least a third party, said method comprising the steps of:

adding encrypted security information pertaining to the first party to a security document created by one of the first, second and third parties;

requiring said security document to be presented to the first party by one of the second and third parties prior to permitting the communication of confidential information;

determining that said security document includes encrypted security information pertaining to each of the first, second and third parties in order to verify that said security document is valid; and

permitting the communication of confidential information of the second party with the third party only after verifying that said security document is valid.

31. A method according to claim 30, wherein said security document is an electronic document, said encrypted security information being added electronically, and the confidential information being communicated electronically.

32. A method according to claim 30, further including the step of requiring an expiration time to be added to said security document, and permitting the communication of confidential information of the second party only if said expiration time has not passed.

33. A method according to claim 32, wherein said expiration time is added electronically.

34. A method according to claim 31, including the step of requiring a preselected expiration time to be added to said security document after at least one of the other parties has added another preselected expiration time, and communicating the confidential information only if the earliest expiration time has not passed.

35. A method according to claim 34, wherein said expiration time is added electronically.

36. A method according to claim 30, wherein said at least a portion of said document is symmetrically encrypted.

37. A method according to claim 30, wherein said at least a portion of said document is asymmetrically encrypted.

38. A method according to claim 30, wherein said encryption information is capable of being decrypted using an encryption key.

39. A method according to claim 38, wherein said encryption key is a public key.

40. A method according to claim 38, wherein said encryption key is a private key.

41. A computer-readable medium for securely communicating confidential information among at least three consenting parties, the computer-readable medium having computer-executable instructions thereon for performing the steps of:

establishing a relationship among the parties;

creating a document initiated by one of the parties;

receiving verifying information about each of the parties;

adding said verifying information to said document in order to validate said document;

presenting said document from at least one of the parties to at least one other of the parties prior to communication of the confidential information therebetween; and

preventing said other of the parties from permitting said communication of the confidential information unless said document is valid.

42. A computer-readable medium according to claim 41, further comprising computer-executable instructions thereon for performing the steps of receiving and adding a preselected expiration time to said document in order to validate said document, and preventing said other of the parties from permitting said communication if said expiration time has passed.

43. A computer-readable medium according to claim 41, further comprising computer-executable instructions thereon for performing the steps of receiving and adding a preselected expiration time from each of at least two of the parties to said document in order to validate said document, and preventing said other of the parties from permitting said communication if the earliest expiration time has passed.

44. A computer-readable medium according to claim 41, wherein at least a portion of said document is encrypted.

45. A computer-readable medium according to claim 44, wherein at least a portion of said document is symmetrically encrypted.

46. A computer-readable medium according to claim 41, wherein at least a portion of said document is asymmetrically encrypted.

47. A computer-readable medium according to claim 41, wherein said document includes a digital signature of each of the at least three parties.

48. A computer-readable medium according to claim 44, wherein said encrypted information is capable of decryption using an encrypted key.

49. A computer-readable medium according to claim 48, wherein said encryption key is a public key.

50. A computer-readable medium according to claim 48, wherein said encryption key is a private key.

51. A computer-readable medium according to claim 50, wherein said private key is a multiple-use key.

52. A computer-readable medium method according to claim 50, wherein said private key is a one-time use key.

53. A computer-readable medium for electronically communicating secure confidential information among at least three consenting parties, the computer-readable medium having computer-executable instructions thereon for performing the steps of:

establishing an electronic communication relationship among all the parties;

creating an electronic ticket initiated by a first of the parties;

adding a digital signature of the first party and encrypted security information pertaining to the first party to said electronic ticket;

adding a digital signature of the second party and encrypted security information pertaining to the second party to said electronic ticket;

adding a digital signature of the third party and encrypted security information pertaining to the third party to said electronic ticket;

validating said electronic ticket by verifying said security information pertaining to said at least three parties;

presenting said electronic ticket from at least one of the parties to another of the parties prior to communicating confidential information therebetween;

and preventing said other of the parties from permitting said communication of confidential information therebetween if said electronic ticket is not validated.

54. A computer-readable medium according to claim 53, further comprising computer-executable instructions thereon for performing the steps of adding a preselected expiration time from at least one of the parties to said electronic ticket in order to validate said electronic ticket, and preventing said other of the parties from permitting said communication of confidential information if said expiration time has passed.

55. A computer-readable medium according to claim 53, further comprising computer-executable instructions thereon for performing the steps of adding a preselected expiration time from each of at least two of the parties to said electronic ticket in order to validate said electronic ticket, and preventing said other of the parties from permitting said communication of confidential information therebetween if the earliest of said expiration times has passed.

56. A computer-readable medium according to claim 53, wherein at least part of said electronic ticket is symmetrically encrypted.

57. A computer-readable medium according to claim 53, wherein at least part of said electronic ticket is asymmetrically encrypted.

58. An apparatus for electronically communicating secure confidential information among at least three parties, said apparatus comprising:

means for establishing an electronic communication relationship among all the parties;

means for creating an electronic ticket initiated by a first of the parties;

means for adding a digital signature of the first party and encrypted security information pertaining to the first party to said electronic ticket;

means for adding a digital signature of the second party and encrypted security information pertaining to the second party to said electronic ticket;

means for adding a digital signature of the third party and encrypted security information pertaining to the third party to said electronic ticket;

means for validating said electronic ticket by verifying said security information pertaining to said at least three parties;

means for presenting said electronic ticket from at least one of the parties to another of the parties prior to communicating confidential information therebetween; and

means for preventing said other of the parties from permitting said communication of confidential information therebetween if said electronic ticket is not validated.

59. An apparatus according to claim 58, further comprising means for adding a preselected expiration time from at least one of the parties to said electronic ticket in order to validate said electronic ticket, and preventing said other of the parties from permitting said communication of confidential information if said expiration time has passed.

60. An apparatus according to claim 58, further comprising means for adding a preselected expiration time from each of at least two of the parties to said electronic ticket in order to validate said electronic ticket, and preventing said other of the parties from permitting said communication of confidential information therebetween if the earliest of said expiration times has passed.

61. An apparatus according to claim 58, wherein at least part of said encrypted security information is symmetrically encrypted.

62. An apparatus according to claim 58, wherein at least part of said encrypted security information is asymmetrically encrypted.

63. A method according to claim 58, wherein said encrypted security information is capable of decryption using an encrypted key.

64. A method according to claim 63, wherein said encryption key is a public key.

65. A method according to claim 63, wherein said encryption key is a private key.

66. A method according to claim 65, wherein said private key is a multiple-use key.

67. A method according to claim 65, wherein said private key is a one-time use key.

68. An apparatus for electronically communicating secure confidential information among at least three parties, said apparatus comprising:

at least one computer having at least one processor that processes data and executes instructions, at least one data storage device that stores data, and at least one memory device that stores instructions and other data, said instructions in said memory device causing said processor to:

establish an electronic communication relationship among all the parties;

create an electronic ticket initiated by a first of the parties;

add a digital signature of the first party and encrypted security information pertaining to the first party to said electronic ticket;

add a digital signature of the second party and encrypted security information pertaining to the second party to said electronic ticket;

add a digital signature of the third party and encrypted security information pertaining to the third party to said electronic ticket;

validate said electronic ticket by verifying said security information pertaining to said at least three parties;

present said electronic ticket from at least one of the parties to another of the parties prior to communicating confidential information therebetween; and

prevent said other of the parties from permitting said communication of confidential information therebetween if said electronic ticket is not validated.

69. An apparatus according to claim 68, wherein said instructions in said memory device further cause to add a preselected expiration time from at least one of the parties to said electronic ticket in order to validate said electronic ticket, and to prevent said other of the parties from permitting said communication of confidential information if said expiration time has passed.

70. An apparatus according to claim 68, wherein said instructions in said memory device further cause to add a preselected expiration time from each of at least two of the parties to said electronic ticket in order to validate said electronic ticket, and to prevent said other of the parties from permitting said communication of confidential information therebetween if the earliest of said expiration times has passed.

71. An apparatus according to claim 68, wherein at least part of said encrypted security information is symmetrically encrypted.

72. An apparatus according to claim 68, wherein at least part of said encrypted security information is asymmetrically encrypted.

73. A method according to claim 68, wherein said encrypted security information is capable of decryption using an encrypted key.

74. A method according to claim 73, wherein said encryption key is a public key.

75. A method according to claim 73, wherein said encryption key is a private key.

76. A method according to claim 75, wherein said private key is a multiple-use key.

77. A method according to claim 75, wherein said private key is a one-time use key.

78. A method of securely communicating confidential information among at least three consenting parties, said method comprising:

establishing a relationship among the parties;

creating a document initiated by one of the parties;

adding verifying information to said document about each of the parties to said document in order to validate said document, at least a portion of said document being encrypted;

at least one of the parties presenting said document to at least one other of the parties prior to communication of the confidential information therebetween; and

said other of the parties permitting said communication of the confidential information therebetween only if said document is valid.

79. A method according to claim 78, further comprising adding an expiration time to said document in order to validate said document, said other of the parties permitting said communication therebetween only if said expiration time has not passed.

80. A method according to claim 78, wherein at least two of the parties add respective preselected expiration times to said document in order to validate said document, said other of the parties permitting said communication therebetween only if the earliest expiration time has not passed.

81. A method according to claim 78, wherein at least a portion of said document is symmetrically encrypted.

82. A method according to claim 78, wherein at least a portion of said document is asymmetrically encrypted.

83. A method according to claim 78, wherein said document includes a digital signature of each of the parties.

84. A method according to claim 78, wherein said encrypted information is capable of decryption using an encryption key.

85. A method according to claim 84, wherein said encryption key is a public key.

86. A method according to claim 84, wherein said encryption key is a private key.

87. A method according to claim 86, wherein said private key is a multiple-use key.

89. A method according to claim 86, wherein said private key is a one-time use key.

90. A method according to claim 78, wherein said encrypted information is encrypted with a public key and capable of decryption using a private key.